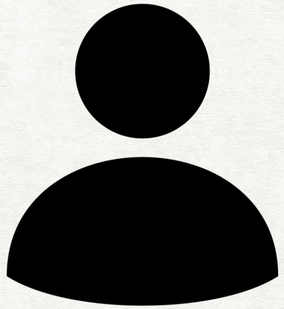
WHAT IS OAUTH?

QUICK HISTORY LESSON

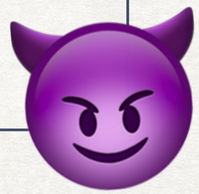
BACK IN THE BAD OLD DAYS

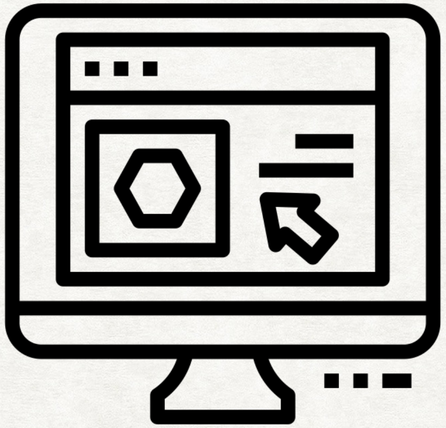


Hey user, would you like me to connect to your MySpace and post updates on your behalf?

Sure, how do I set that up?

Easy! Just
give me your MySpace password!
I promise not to
do anything bad with it…





OAuth is a protocol that

allows users to

authorize (or "connect accounts")

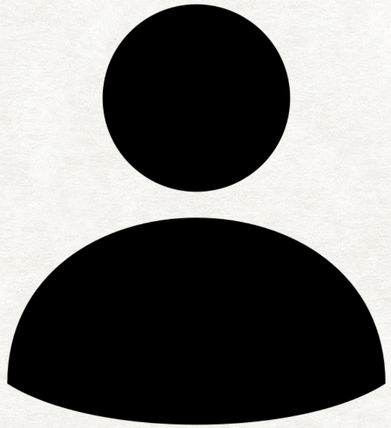
from one website

to another,

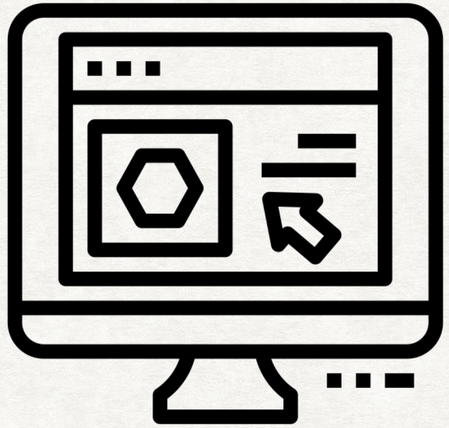
without sharing passwords.

HOW DO I OAUTH?

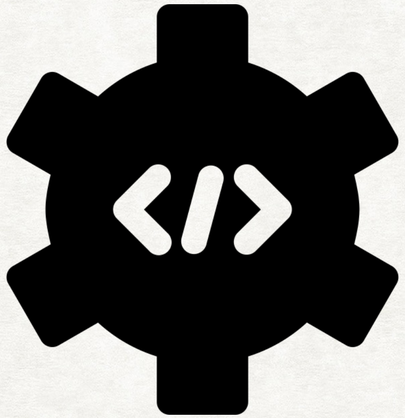
THREE ROLES INVOLVED



User

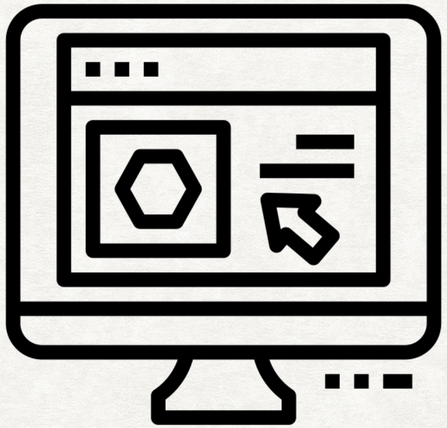


API Consumer



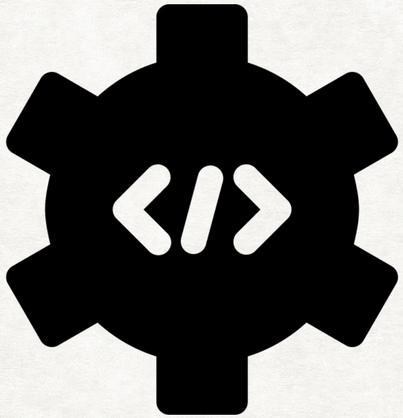
API Provider

SETUP: CONSUMER REGISTERS WITH PROVIDER

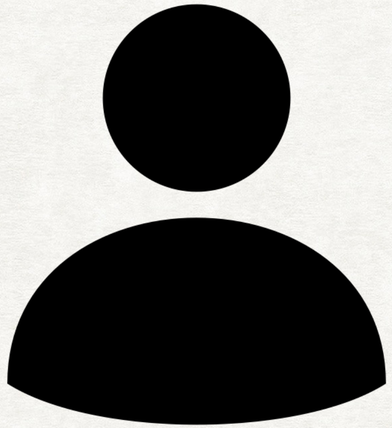


Hi, I'd like to use your API to get information about your users.

I'm OK with that if the users are.
Here's your API key & secret.
If you use this API for bad things,
I'll revoke them to
disable your API access!

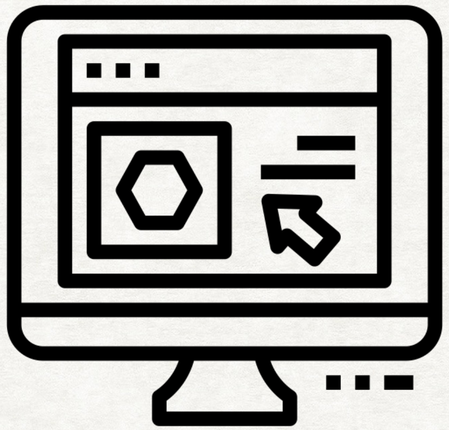


STEP 1: USER ARRIVES AT CONSUMER

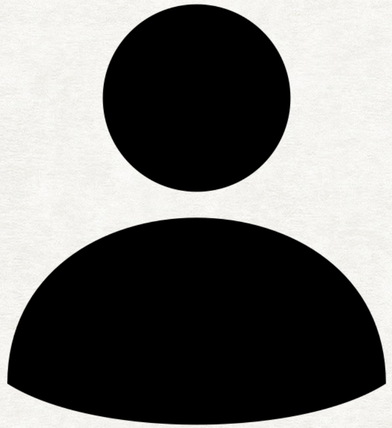


Oh, looks like I can login with Google! I'd like to do that, please.

In order to log you in, I need to ask Google who you are. Google won't tell me anything about you unless you give permission, so I'm going to send you to Google now.



STEP 2: USER REDIRECTED TO PROVIDER



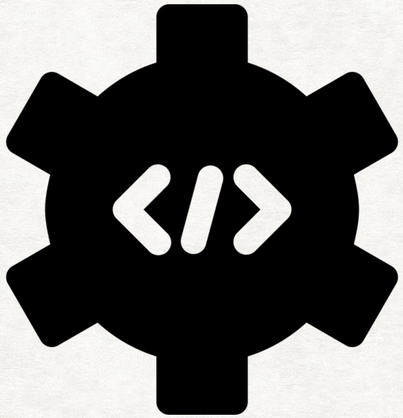
Looks like this other website wants to know some of your information. Is that OK with you?

What do they want to know?

They just want your email address.

Oh sure, that's fine.

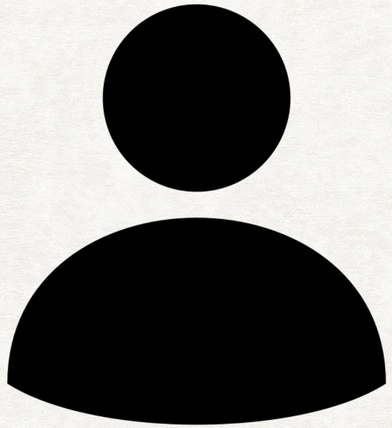
OK, I'll give you this secret code, and send you back to the site. They'll know what to do with the code.



CODE

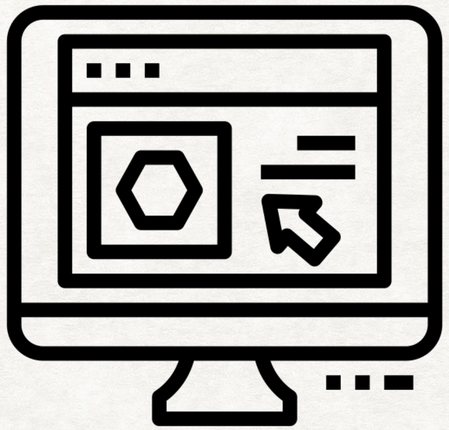
STEP 3: USER GIVES CODE TO CONSUMER

CODE



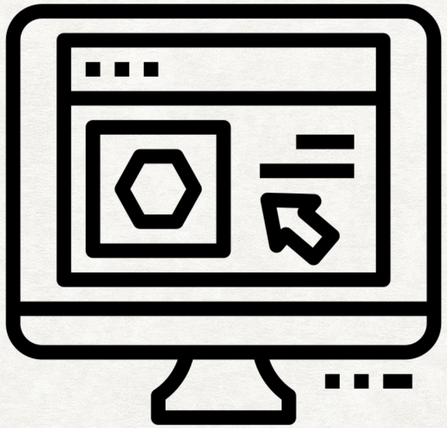
Alright, I talked to Google, and they gave me this secret code. Can I log in now?

Perfect! Just give me a second, and then you can log in…



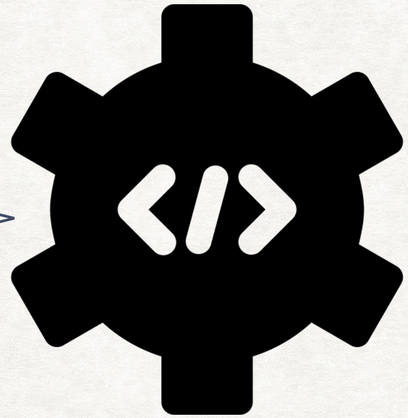
STEP 4: CONSUMER EXCHANGES CODE FOR TOKEN

CODE



This code proves that the user gave permission to let me see their data.

Yep, that code matches the one I just gave the user! OK, I'm willing to give you the data that the user approved. That secret code was just temporary, though: take this token instead, and store it as securely as you would store the user's password!

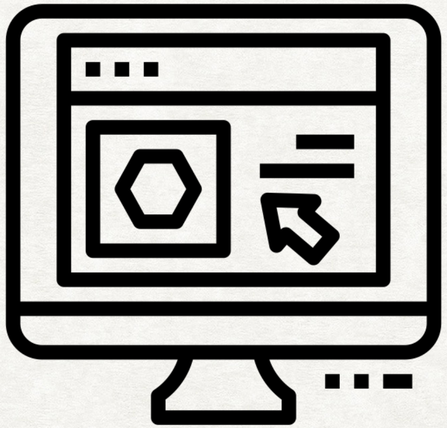


TOKEN

STEP 5: CONSUMER MAKES API REQUESTS

TOKEN

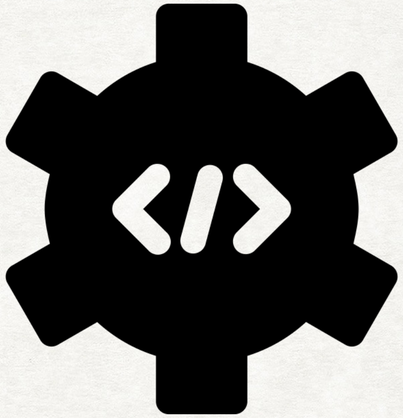
I'd like the user's email address, please. Here's my token.



Let's see…

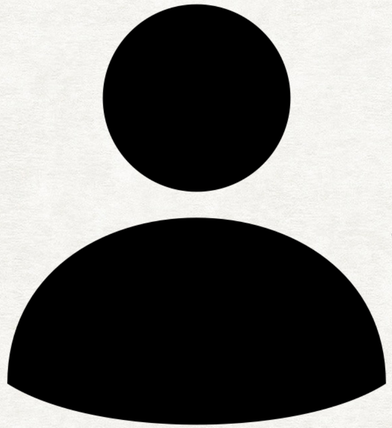
- Valid API token?
- Matches an active user I know about?
- Consumer's API access has not been revoked?
- User has not revoked permission?
- Data requested matches what user allowed?

Yep, looks good! Here's the data you asked for:

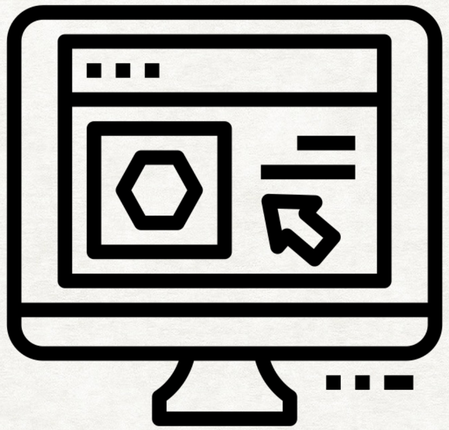


EMAIL

RESULT: SMOOTH INTEGRATION



I got your email from Google, so now I know who you are. You can login now!

Yay, that was easy!

Actually, it was really complicated, but I'm glad it looked easy to you 😅